MIMO Beamforming for Secure and Energy-Efficient Wireless Communication

Nguyen T. Nghia[1], Hoang D. Tuan[1], Trung Q. Duong[2] and H. Vincent Poor[3]

***Abstract*—Considering a multiple-user multiple-input multiple-output (MIMO) channel with an eavesdropper, this letter develops a beamformer design to optimize the energy efficiency in terms of secrecy bits per Joule under secrecy quality-of-service constraints. This is a very difficult design problem with no available exact solution techniques. A path-following procedure, which iteratively improves its feasible points by using a simple quadratic program of moderate dimension, is proposed. Under any fixed computational tolerance the procedure terminates after finitely many iterations, yielding at least a locally optimal solution. Simulation results show the superior performance of the obtained algorithm over other existing methods.**

***Index Terms*—MIMO beamforming, secure communication, energy efficiency.**

I. Introduction

Secure communication achieved by exploiting the wireless physical layer to provide secrecy in data transmission, has drawn significant recent research attention (see e.g. [1]–[3] and references therein). The performance of this type of secure communication can be measured in terms of the secrecy throughput, which is the capacity of conveying information to the intended users while keeping it confidential from eavesdroppers [2], [4]. On the other hand, energy efficiency (EE) has emerged as another important figure-of-merit in assessing the performance of communication systems [5], [6]. For most systems, both security and energy efficiency are of interest, and thus it is of interest to combine these two metrics into a single performance index called the secrecy EE (SEE), which can be expressed in terms of secrecy bits per Joule.

Transmit beamforming can be used to enhance the two conflicting targets for optimizing SEE in multiple-user multiple-input multiple-output (MU-MIMO) communications: mitigating MU interference to maximize the users' information throughput, and jamming eavesdroppers to control the leakage of information. However, the current approach to treat both EE [7], [8] and SEE [9], [10] is based on costly zero-forcing beamformers, which completely cancel the MU interference and signals received at the eavesdroppers. The EE/SEE objective is in the form of a ratio of a concave function and a convex function, which can be optimized by using Dinkelbach's algorithm [11]. Each Dinkelbach's iteration still requires a log-det function optimization, which is convex but computationally quite complex. Moreover, zero-forcing beamformers are mostly suitable for low code rate applications and are applicable to specific MIMO systems only. The computational complexity of SEE for single-user MIMO/SISO communications as considered in [12] and [13] is also high as each iteration still involves a difficult nonconvex optimization problem.

This letter aims to design transmit beamformers to optimize SEE subject to per-user secrecy quality-of-service (QoS) and transmit power constraints. The specific contributions are detailed in the following dot-points.

- A path-following computational procedure, which invokes a simple convex quadratic program at each iteration and converges to at least a locally optimal solution, is proposed. The MU interference and eavesdropped signals are effectively suppressed for optimizing the SEE. In contrast to zero-forcing beamformers, higher code rates not only result in transmitting more concurrent data streams but also lead to much better SEE performance in our proposed beamformer design.
- As a by-product, other important problems in secure and energy-efficient communications, such as EE maximization subject to the secrecy level or sum secrecy throughput maximization, which are still quite open for research, can be effectively addressed by the proposed procedure.

Notation. All variables are written in boldface. For illustrative purpose, $f(\mathbf{V})$ is a mapping of variable $\mathbf{V}$ while $f(\bar{V})$ is the output of mapping f corresponding to a particular input $\bar{V}$. I_n denotes the identity matrix of size $n \times n$. The notation $(\cdot)^H$ stands for the Hermitian transpose, $|A|$ denotes the determinant of a square matrix A, and $\langle A \rangle$ denotes its trace while $(A)^2 = AA^H$. The inner product $\langle X, Y \rangle$ is defined as $\langle X^H Y \rangle$ and therefore the Frobenius squared norm of a matrix X is $||X||^2 = \langle XX^H \rangle$. The notation $A \succeq B$ ($A \succ B$, respectively) means that $A - B$ is a positive semidefinite (definite, respectively) matrix. $\mathbb{E}[\cdot]$ denotes expectation and $\Re\{\cdot\}$ denotes the real part of a complex number. $\mathcal{CN}(0, a)$ denotes a circularly-symmetric complex Gaussian random variable with mean zero and variance a.

II. SEE Formulation

Consider a MIMO system consisting of D transmitters and D users indexed by $1, \ldots, D$. Each transmitter j is equipped with N antennas to transmit information to its intended user j equipped with N_r antennas. There is an eavesdropper equipped with N_e antennas, which is part of the legitimate network [1], [4]. The channel matrices $H_{\ell j} \in \mathbb{C}^{N_r \times N}$ and $H_{\ell e} \in \mathbb{C}^{N_e \times N}$

This work was supported in part by the Australian Research Councils Discovery Projects under Project DP130104617, in part by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415/14/22, and in part by the U.S. National Science Foundation under Grants CMMI-1435778 and ECCS-1647198.

[1]Faculty of Engineering and Information Technology, University of Technology, Sydney, NSW 2007, Australia (email: nghia.t.nguyen@student.uts.edu.au, tuan.hoang@uts.edu.au).

[2]The School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast BT7 1NN, United Kingdom (e-mail: trung.q.duong@qub.ac.uk).

[3]Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu).

from transmitter ℓ to user j and to the eavesdropper, respectively, are known at the transmitters by using the channel reciprocity, feedback and learning mechanisms [1], [4], [14], [15].

A complex-valued vector $s_j \in \mathbb{C}^{d_1}$ contains the information transmitter j intends to convey to user j, where $\mathbb{E}\left[s_j s_j^H\right] = I_{d_1}$, and $d_1 \leq N$ is the number of concurrent data streams. Denote by $\mathbf{V}_j \in \mathbb{C}^{N\times d_1}$ the complex-valued beamformer matrix for user j. The ratio d_1/N is called the code rate of $\mathbf{V}_j$. For notational convenience, define $\mathcal{D} \triangleq \{1,\ldots,D\}$ and $\mathbf{V} \triangleq [\mathbf{V}_j]_{j\in\mathcal{D}}$.

The received signal at user j and the signal received at the eavesdropper are

$$y_j = H_{jj}\mathbf{V}_j s_j + \sum_{\ell\in\mathcal{D}\setminus\{j\}} H_{\ell j}\mathbf{V}_\ell s_\ell + \tilde{n}_j, \quad (1)$$

$$y_e = \sum_{j=1}^{D} H_{je}\mathbf{V}_j s_j + \tilde{n}_e, \quad (2)$$

where $\tilde{n}_j \in \mathcal{CN}(0,\sigma_j^2)$ and $\tilde{n}_e \in \mathcal{CN}(0,\sigma_e^2)$ are additive noises.

By (1), the rate of information f_j leaked from user j (in nats) is

$$f_j(\mathbf{V}) = \ln\left|I_{N_r} + (\mathcal{L}_j(\mathbf{V}_j))^2(\Psi_j(\mathbf{V}) + \sigma_j^2 I_{N_r})^{-1}\right|, \quad (3)$$

where $\mathcal{L}_j(\mathbf{V}_j) \triangleq H_{jj}\mathbf{V}_j$ and $\Psi_j(\mathbf{V}) \triangleq \sum_{\ell\in\mathcal{D}\setminus\{j\}}(H_{\ell j}\mathbf{V}_\ell)^2$. On the other hand, the wiretapped throughput for user j at the eavesdropper is

$$f_{j,e}(\mathbf{V}) \triangleq \ln\left|I_{N_e} + (\mathcal{L}_{j,e}(\mathbf{V}_j))^2(\Psi_{j,e}(\mathbf{V}) + \sigma_e^2 I_{N_e})^{-1}\right|, \quad (4)$$

where $\mathcal{L}_{j,e}(\mathbf{V}_j) \triangleq H_{je}\mathbf{V}_j$ and $\Psi_{j,e}(\mathbf{V}) \triangleq \sum_{\ell\in\mathcal{D}\setminus\{j\}}(H_{\ell e}\mathbf{V}_\ell)^2$. The secrecy throughput in transmitting information s_j to user j while keeping it confidential from the eavesdropper is defined as [2], [4]

$$f_{j,s}(\mathbf{V}) \triangleq f_j(\mathbf{V}) - f_{j,e}(\mathbf{V}). \quad (5)$$

Following [16], the consumed power for signal transmission is modelled by $P^{\rm tot}(\mathbf{V}) \triangleq \zeta P^t(\mathbf{V}) + P_c$, where $P^t(\mathbf{V}) \triangleq \sum_{j=1}^{D}||\mathbf{V}_j||^2$ is the total transmit power of the transmitters and ζ and P_c are the reciprocal of the drain efficiency of the power amplifier and the circuit power, respectively.

Consider the following secure beamformer design to optimize the system's energy efficiency:

$$\max_{\mathbf{V}} \ \frac{1}{P^{\rm tot}(\mathbf{V})}\sum_{j=1}^{D}(f_j(\mathbf{V}) - f_{j,e}(\mathbf{V})) \quad \text{s.t.} \quad (6a)$$

$$||\mathbf{V}_j||^2 \leq P_{\max},\ j\in\mathcal{D}, \quad (6b)$$

$$f_j(\mathbf{V}) - f_{j,e}(\mathbf{V}) \geq r_j, j\in\mathcal{D}, \quad (6c)$$

where the constraints (6b) limit the transmit power, while (6c) are the secrecy QoS constraints.

It can be seen from their definitions (3) and (4) that both throughput f_j and wiretapped throughput $f_{j,e}$ are very complicated functions of the beamformer variable $\mathbf{V}$. The approach of [7] and [8] (to EE) and [9] and [10] (to SEE) seeks $\mathbf{V}$ in the class of zero-forcing beamformers $\Psi_j(\mathbf{V}) \equiv 0$, $j\in\mathcal{D}$ and $\sum_{\ell\in\mathcal{D}}(H_{\ell e}\mathbf{V}_\ell)^2 \equiv 0$ to cancel completely all the MU interference and wiretapped signals. Each throughput f_j becomes a log-det function of only $\mathbf{V}_j$. Dinkelbach's algorithm is then applied to compute a zero-forcing solution of (6), which requires a log-det function optimization for each iteration. Such optimization is still computationally difficult with no available polynomial-time solvers. Note that the feasibility of the zero-forcing constraints imposes $N \geq N_e + d_1$ and $D(N + N_r - N_e - 2d_1) \geq (D-1)d_1$ [10]. Thus, there is not much freedom for optimizing zero-forcing beamformers whenever N is not large.

In the next section, we will provide a completely new computational approach to (6) by effectively enhancing its difficult objective and constraints.

III. Path-following computational procedure

By introducing a variable $\mathbf{t}$ satisfying the convex quadratic constraint

$$\zeta\sum_{j=1}^{D}||\mathbf{V}_j||^2 + P^{\rm BS} \leq \mathbf{t}, \quad (7)$$

the optimization problem (6) can be equivalently expressed as

$$\max_{\mathbf{V},\mathbf{t}} \ \mathcal{P}(\mathbf{V},\mathbf{t}) \triangleq \frac{1}{\mathbf{t}}\sum_{j=1}^{D}(f_j(\mathbf{V}) - f_{j,e}(\mathbf{V})) \text{ s.t. } (6b),(6c). \quad (8)$$

In what follows, a function h is said to be a *minorant* (*majorant*, resp.) of a function f at a point $\bar{x}$ in the definition domain $\mathrm{dom}(f)$ of f iff $h(\bar{x}) = f(\bar{x})$ and $h(\mathbf{x}) \leq f(\mathbf{x})\ \forall\ \mathbf{x}\in\mathrm{dom}(f)$ ($h(\mathbf{x}) \geq f(\mathbf{x})\ \forall\ \mathbf{x}\in\mathrm{dom}(f)$, resp.) [17].

By [18], a *concave quadratic minorant* of the throughput function $f_j(\mathbf{V})$ at $V^{(\kappa)} \triangleq [V_j^{(\kappa)}]_{j\in\mathcal{D}}$, which is feasible for (6b)-(6c) is

$$\Theta_j^{(\kappa)}(\mathbf{V}) \triangleq a_j^{(\kappa)} + 2\Re\{\mathcal{A}_j^{(\kappa)}, \mathcal{L}_j(\mathbf{V}_j)\rangle\} - \langle\mathcal{B}_j^{(\kappa)}, \mathcal{M}_j(\mathbf{V})\rangle, \quad (9)$$

where $\mathcal{M}_j(\mathbf{V}) \triangleq \Psi_j(\mathbf{V}) + (\mathcal{L}_j(\mathbf{V}_j))^2$, $0 > a_j^{(\kappa)} \triangleq f_j(V^{(\kappa)}) - \langle(\mathcal{L}_j(V_j^{(\kappa)}))^H(\Psi_j(V^{(\kappa)}) + \sigma_j^2 I_{N_r})^{-1}\mathcal{L}_j(V_j^{(\kappa)})\rangle - \sigma_j^2\langle(\Psi_j(V^{(\kappa)}) + \sigma_j^2 I_{N_r})^{-1} - (\mathcal{M}_j(V^{(\kappa)}) + \sigma_j^2 I_{N_r})^{-1}\rangle$, $\mathcal{A}_j^{(\kappa)} \triangleq (\Psi_j(V^{(\kappa)}) + \sigma_j^2 I_{N_r})^{-1}\mathcal{L}_j(V_j^{(\kappa)})$ and

$$0 \preceq \mathcal{B}_j^{(\kappa)} \triangleq (\Psi_j(V^{(\kappa)}) + \sigma_j^2 I_{N_r})^{-1} - (\mathcal{M}_j(V^{(\kappa)}) + \sigma_j^2 I_{N_r})^{-1}.$$

To provide a minorant of the secrecy throughput $f_{j,s}$ (see (5)) at $V^{(\kappa)}$, the next step is to find a *majorant* of the eavesdropper throughput function $f_{j,e}(\mathbf{V})$ at $V^{(\kappa)}$. Reexpressing $f_{j,e}$ by

$$\ln\left|I_{N_e} + \mathcal{M}_{j,e}(\mathbf{V})/\sigma_e^2\right| - \ln\left|I_{N_e} + \Psi_{j,e}(\mathbf{V})/\sigma_e^2\right|, \quad (10)$$

for $\mathcal{M}_{j,e}(\mathbf{V}) \triangleq \Psi_{j,e}(\mathbf{V}) + (\mathcal{L}_{j,e}(\mathbf{V}_j))^2$, and applying Theorem 1 in the appendix for upper bounding the first term and lower bounding the second term in (10) yields the following *convex quadratic majorant* of $f_{j,e}$ at $V^{(\kappa)}$:

$$\Theta_{j,e}^{(\kappa)}(\mathbf{V}) \triangleq a_{j,e}^{(\kappa)} - 2\sum_{\ell\in\mathcal{D}\setminus\{j\}}\Re\{\langle H_{\ell e}V_\ell^{(\kappa)}\mathbf{V}_\ell^H H_{\ell e}^H\rangle\}/\sigma_e^2 + \langle\mathcal{B}_{j,e1}^{(\kappa)}, \mathcal{M}_{j,e}(\mathbf{V})\rangle/\sigma_e^2 + \langle\mathcal{B}_{j,e2}^{(\kappa)}, \Psi_{j,e}(\mathbf{V})\rangle/\sigma_e^2,$$

where $a_{j,e}^{(\kappa)} \triangleq f_{j,e}(V^{(\kappa)}) + \langle(I_{N_e} + \mathcal{M}_{j,e}(V^{(\kappa)})/\sigma_e^2)^{-1} - I_{N_e} + \Psi_{j,e}(V^{(\kappa)})/\sigma_e^2\rangle$, and

$$0 \preceq \mathcal{B}_{j,e1}^{(\kappa)} \triangleq (I_{N_e} + \mathcal{M}_{j,e}(V^{(\kappa)})/\sigma_e^2)^{-1},$$
$$0 \preceq \mathcal{B}_{j,e2}^{(\kappa)} \triangleq (\sigma_e^2)^{-1}I_{N_e} - (\sigma_e^2 I_{N_e} + \Psi_{j,e}(V^{(\kappa)}))^{-1}.$$

A *concave quadratic minorant* of the secrecy throughput function $f_{j,s}$ at $V^{(\kappa)}$ is then

$$\begin{aligned}\Theta_{j,s}^{(\kappa)}(\mathbf{V}) &= \Theta_{j}^{(\kappa)}(\mathbf{V}) - \Theta_{j,e}^{(\kappa)}(\mathbf{V}) \\ &= a_{j,s}^{(\kappa)} + \mathcal{A}_{j,s}^{(\kappa)}(\mathbf{V}) - \mathcal{B}_{j,s}^{(\kappa)}(\mathbf{V}). \end{aligned} \quad (11)$$

Here, $a_{j,s}^{(\kappa)} \triangleq a_{j}^{(\kappa)} + a_{j,e}^{(\kappa)}$, $\mathcal{A}_{j,s}^{(\kappa)}(\mathbf{V}) \triangleq 2\Re\{\langle \mathcal{A}_{j}^{(\kappa)}, \mathcal{L}_j(\mathbf{V}_j)\rangle\} + 2\sum_{\ell\in\mathcal{D}\setminus\{j\}} \Re\{\langle H_{\ell e} V_{\ell}^{(\kappa)} \mathbf{V}_{\ell}^H H_{\ell e}^H\rangle\}/\sigma_e^2$, and $\mathcal{B}_{j,s}^{(\kappa)}(\mathbf{V}) \triangleq \langle \mathcal{B}_{j}^{(\kappa)}, \mathcal{M}_j(\mathbf{V})\rangle + \langle \mathcal{B}_{j,e1}^{(\kappa)}, \mathcal{M}_{j,e}(\mathbf{V})\rangle + \langle \mathcal{B}_{j,e2}^{(\kappa)}, \Psi_{j,e}(\mathbf{V})\rangle/\sigma_e^2$.

Therefore, the nonconvex secrecy QoS constraints (6c) can be innerly approximated by the following convex quadratic constraints in the sense that the feasibility of the former is guaranteed by the feasibility of the latter:

$$\Theta_{j,s}^{(\kappa)}(\mathbf{V}) \geq r_j, j = 1, ..., D. \quad (12)$$

For good approximation, the following trust region is imposed:

$$\mathcal{A}_{j,s}^{(\kappa)}(\mathbf{V}) \quad \geq \quad 0, \ j = 1, ..., D. \quad (13)$$

By using the inequality

$$\frac{x}{t} \geq 2\frac{\sqrt{x^{(\kappa)}}\sqrt{x}}{t^{(\kappa)}} - \frac{x^{(\kappa)}}{(t^{(\kappa)})^2}t \quad \forall x > 0, x^{(\kappa)} > 0, t > 0, t^{(\kappa)} > 0$$

we obtain $\mathcal{A}_{j,s}^{(\kappa)}(\mathbf{V})/\mathbf{t} \geq \varphi_{j,s}^{(\kappa)}(\mathbf{V}, \mathbf{t})$, for

$$\varphi_{j,s}^{(\kappa)}(\mathbf{V}, \mathbf{t}) \triangleq 2b_{j,s}^{(\kappa)}\sqrt{\mathcal{A}_{j,s}^{(\kappa)}(\mathbf{V})} - c_{j,s}^{(\kappa)}\mathbf{t} \quad (14)$$

where $0 < b_{j,s}^{(\kappa)} \triangleq \sqrt{\mathcal{A}_{j,s}^{(\kappa)}(V^{(\kappa)})}/t^{(\kappa)}$, $0 < c_{j,s}^{(\kappa)} \triangleq (b_{j,s}^{(\kappa)}/t^{(\kappa)})^2$, which is a concave function [17].

With regard to $a_{j,s}^{(\kappa)}/\mathbf{t}$ we define a concave function $a_{j,s}^{(\kappa)}(\mathbf{t})$ as follows:

- If $a_{j,s}^{(\kappa)} < 0$, define $a_{j,s}^{(\kappa)}(\mathbf{t}) \triangleq a_{j,s}^{(\kappa)}/\mathbf{t}$, which is a concave function;
- If $a_{j,s}^{(\kappa)} > 0$, define $a_{j,s}^{(\kappa)}(\mathbf{t}) = a_{j,s}^{(\kappa)}(2/t^{(\kappa)} - \mathbf{t}/(t^{(\kappa)})^2)$, which is a linear minorant of the convex function $a_{j,s}^{(\kappa)}/\mathbf{t}$ at $t^{(\kappa)}$.

A *concave minorant* of $\Theta_{j,s}^{(\kappa)}(\mathbf{V})/\mathbf{t}$, which is also a minorant of $(f_j(\mathbf{V}) - f_{j,e}(\mathbf{V}))/\mathbf{t}$ at $(V^{(\kappa)}, t^{(\kappa)})$, is thus

$$g_{j,s}^{(\kappa)}(\mathbf{V}, \mathbf{t}) \triangleq a_{j,s}^{(\kappa)}(\mathbf{t}) + \varphi_{j}^{(\kappa)}(\mathbf{V}_j, \mathbf{t}) - \mathcal{B}_{j,s}^{(\kappa)}(\mathbf{V})\rangle/\mathbf{t}. \quad (15)$$

We now solve the nonconvex optimization problem (6) by generating the next feasible point $(V^{(\kappa+1)}, t^{(\kappa)})$ as the optimal solution of the following convex quadratic program (QP), which is an inner approximation [17] of the nonconvex optimization problem (8):

$$\begin{aligned}\max_{\mathbf{V},\mathbf{t}} \ & \mathcal{P}^{(\kappa)}(\mathbf{V}, \mathbf{t}) \triangleq \sum_{j=1}^{D} g_{j,s}^{(\kappa)}(\mathbf{V}, \mathbf{t}) \\ & \text{s.t.} \quad (6b), (7), (12), (13). \end{aligned} \quad (16)$$

Note that (16) involves $n = 2DNd_1 + 1$ scalar real variables and $m = 2D + 1$ quadratic constraints so its computational complexity is $\mathcal{O}(n^2m^{2.5} + m^{3.5})$.

It can be seen that $\mathcal{P}(V^{(\kappa+1)}, t^{(\kappa+1)}) \geq \mathcal{P}^{(\kappa)}(V^{(\kappa+1)}, t^{(\kappa+1)}) > \mathcal{P}^{(\kappa)}(V^{(\kappa)}, t^{(\kappa)}) = \mathcal{P}(V^{(\kappa)}, t^{(\kappa)})$ as long as $(V^{(\kappa+1)}, t^{(\kappa+1)}) \neq (V^{(\kappa)}, t^{(\kappa)})$, i.e. $(V^{(\kappa+1)}, t^{(\kappa+1)})$ is better than $(V^{(\kappa)}, t^{(\kappa)})$. This means that, once initialized from a feasible point $(V^{(0)}, t^{(0)})$ for (8), the κ-th QP iteration (16) generates a sequence $\{(V^{(\kappa)}, t^{(\kappa)})\}$ of feasible and improved points toward the nonconvex optimization problem (8), which converges at least to a locally optimal solution of (6) [18]. Under the stopping criterion

$$\left|\left(\mathcal{P}(V^{(\kappa+1)}, t^{(\kappa+1)}) - \mathcal{P}(V^{(\kappa)}, t^{(\kappa)})\right)/\mathcal{P}(V^{(\kappa)}, t^{(\kappa)})\right| \leq \epsilon$$

for a given tolerance $\epsilon > 0$, the QP iterations will terminate after finitely many iterations.

The proposed path-following procedure for computational solution of the nonconvex optimization problem (6) is summarized in Algorithm 1.

Algorithm 1 Path-following Algorithm for SEE Optimization

Initialization: Set $\kappa := 0$, and choose a feasible point $(V^{(0)}, t^{(0)})$ for (8).

κ-th iteration: Solve (16) for an optimal solution (V^*, t^*) and set $\kappa := \kappa + 1$, $V^{(\kappa)}, t^{(\kappa)}) \triangleq (V^*, t^*)$ and calculate $\mathcal{P}(V^{(\kappa)}, t^{(\kappa)})$. Stop if $\left|\left(\mathcal{P}(V^{(\kappa)}, t^{(\kappa)}) - \mathcal{P}(V^{(\kappa-1)}), t^{(\kappa-1)}\right)/\mathcal{P}(V^{(\kappa-1)}, t^{(\kappa-1)})\right| \leq \epsilon$.

We note that a feasible initial point $(V^{(0)}, t^{(0)})$ for (8) can be found by solving

$$\max_{\mathbf{V}} \min_{j\in\mathcal{D}} \ (f_j(\mathbf{V}) - f_{j,e}(\mathbf{V}))/r_j \quad \text{s.t.} \quad (6b)$$

by the iterations $\left\{\max_{\mathbf{V}} \min_{j\in\mathcal{D}} \ \Theta_{j,s}^{(\kappa)}(\mathbf{V})/r_j \quad \text{s.t.} \quad (6b)\right\}$, which terminate upon reaching $(f_j(V^{(\kappa)}) - f_{j,e}(V^{(\kappa)}))/r_j \geq 1 \ \forall j \in \mathcal{D}$, to satisfy (6b)-(6c).

The following problem of EE optimization under users' throughput QoS constraints and secrecy levels:

$$\begin{aligned}\max_{\mathbf{V}} \ & \frac{1}{P^{\text{tot}}(\mathbf{V})}\sum_{j=1}^{D} f_j(\mathbf{V}) \quad \text{s.t.} \quad (6b), \\ & f_j(\mathbf{V}) \geq r_j \ \& \ f_{j,e}(\mathbf{V}) \leq \epsilon, j = 1, ..., D, \end{aligned} \quad (17)$$

where ϵ is set small enough to keep the users' information confidential from the eavesdropper, is simpler than (6). It can be addressed by a similar path-following procedure, which solves the following QP at the $\kappa-$th iteration instead of (16):

$$\begin{aligned}\max_{\mathbf{V},\mathbf{t}} \sum_{j=1}^{D} \Big(& a_j^{(\kappa)}/\mathbf{t} + 4b_j^{(\kappa)}\sqrt{\Re\{\langle \mathcal{A}_j^{(\kappa)}, \mathcal{L}_j(\mathbf{V}_j)\rangle\}} \\ & -2c_j^{(\kappa)}\mathbf{t} - \langle \mathcal{B}_j^{(\kappa)}, \mathcal{M}_j(\mathbf{V})\rangle/\mathbf{t}\Big) \quad \text{s.t.} \quad (6b), \end{aligned} \quad (18a)$$

$$\Re\{\langle \mathcal{A}_j^{(\kappa)}, \mathcal{L}_j(\mathbf{V}_j)\rangle\} \geq 0, \ j \in \mathcal{D}, \quad (18b)$$

$$\Theta_j^{(\kappa)}(\mathbf{V}) \geq r_j \ \& \ \Theta_{j,e}^{(\kappa)}(\mathbf{V}) \leq \epsilon, \ j \in \mathcal{D}, \quad (18c)$$

where $0 < b_j^{(\kappa)} \triangleq \langle (\mathcal{L}_j(V_j^{(\kappa)}))^H(\Psi_j(V^{(\kappa)}) + \sigma_j^2 I_{N_r})^{-1}\mathcal{L}_j(V_j^{(\kappa)})\rangle^{1/2}/t^{(\kappa)}$, $0 < c_j^{(\kappa)} \triangleq (b_j^{(\kappa)}/t^{(\kappa)})^2$ and $\mathcal{A}_j^{(\kappa)}$ and $\mathcal{B}_j^{(\kappa)}$ are defined from (9). A feasible initial point $(V^{(0)}, t^{(0)})$ for (17) can be found by solving

$$\max_{\mathbf{V}} \min_{j\in\mathcal{D}} \min\{f_j(\mathbf{V}) - r_j, \epsilon - f_{j,e}(\mathbf{V})\} \quad \text{s.t.} \quad (6b)$$

by the iterations

$$\max_{\mathbf{V}} \min_{j\in\mathcal{D}} \min\{\Theta_j^{(\kappa)}(\mathbf{V}) - r_j, \epsilon - \Theta_{j,e}^{(\kappa)}(\mathbf{V})\} \quad \text{s.t.} \quad (6b)\},$$

which terminate upon reaching $f_j(V^{(\kappa)}) - r_j \geq 0$, $\epsilon - f_{j,e}(V^{(\kappa)}) \geq 0\ \forall j \in \mathcal{D}$, to satisfy (6b), (17).

Lastly, the problem of sum secrecy throughput maximization

$$\max_{\mathbf{V}} \sum_{j=1}^{D} (f_j(\mathbf{V}) - f_j(\mathbf{V})) \quad \text{s.t. } (6b), (6c)$$

is also simpler than the SEE optimization problem (6), which can be addressed by a similar path-following procedure with the QP

$$\max_{\mathbf{V}} \sum_{j=1}^{D} \Theta_{j,s}^{(\kappa)}(\mathbf{V}) \text{ s.t. } (6b), (12)$$

solved at the $\kappa-$th iteration instead of (16).

IV. Numerical Examples

The fixed parameters are: $D = 3$, $N = 12$, $N_r = 6$, $N_e = 9$, $\sigma_j \equiv 1$, $\sigma_e = 1$, $r_j \equiv 1$ bits/s/Hz, $\zeta = 1$ and $P_c \in \{7, 10\}$ dB. The secrecy level $\epsilon = 0.05/\log_2 e$ is set in solving (17). The channels are Rayleigh fading so their coefficients are generated as $\mathcal{CN}(0, 1)$.

For the first numerical example, the number of data streams $d_1 = 3$ is set, so the code rate is $3/12 = 1/4$. Each $\mathbf{V}_j$ is of size 12×3. Figure 1 shows the SEE performance of our proposed beamformer and the zero-forcing beamformer [9], [10]. One can see that the former outperforms the latter substantially. Apparently, the latter is not quite suitable for both EE and SEE. The SEE performance achieved by the formulation (6) is better than that achieved by the formulation (17) because the secrecy level is enhanced with the users's throughput in the former instead of being constrained beforehand in the latter. When the transmit power $P_{\max}$ is small, the denominator of the SEE objective in (6) and (17) is dominated by the constant circuit power P_c. As a result, the SEE is maximized by maximizing its numerator, which is the system sum secrecy throughput. On the other hand, the SEE objective is likely maximized by minimizing the transmitted power $P_{\max}$ in its denominator when the latter is dominated by $P_{\max}$. That is why the SEE saturates once $P_{\max}$ is beyond a threshold according to Figure 1. We increase the number d_1 of data streams to 4 in the second

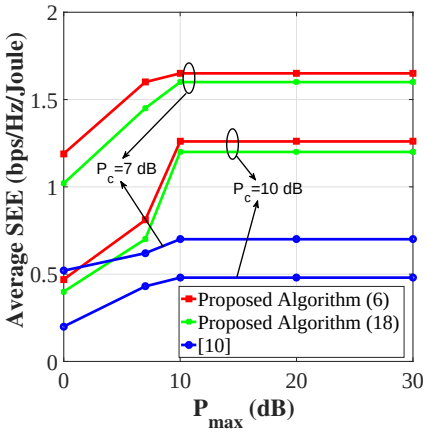

Fig. 1: Average SEE vs. P_{max} for $d_1 = 3$.

numerical example. The code rate is thus $4/12 = 1/3$. For this higher-code-rate case, the zero-forcing beamformers [9], [10] are infeasible. Comparing Figure 1 and Figure 2 reveals that higher code-rate beamforming is also much better in terms of SEE because it leads to greater freedom in designing $\mathbf{V}_j$ of size 12×4 for maximizing the SEE. In other words, the effect of code rate diversity on the SEE is observed.

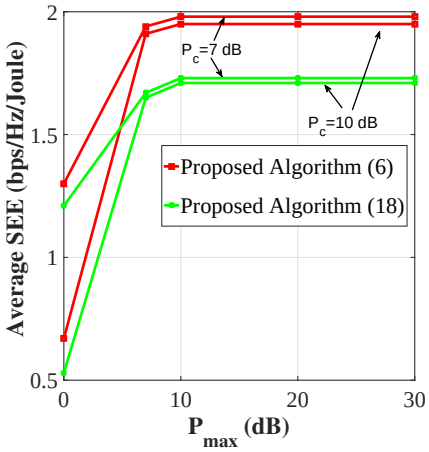

Fig. 2: Average SEE vs. P_{max} for $d_1 = 4$.

V. Conclusion

We have proposed a path-following computational procedure for the beamformer design to maximize the energy efficiency of a secure MU MIMO wireless communication system and have also showed its potential in solving other important optimization problems in secure and energy-efficient communications. Simulation results have confirmed the superior performance of the proposed method over the exiting techniques.

Acknowledgement. The authors thank Dr. H. H. Kha for providing the computational code from [10].

Appendix

Theorem 1: For a given $\sigma > 0$, consider a function

$$f(\mathbf{X}) = \ln |I_m + (\mathbf{X})^2/\sigma|$$

in $\mathbf{X} \in \mathbb{C}^{m \times n}$. Then for any $\bar{X} \in \mathbb{C}^{m \times n}$, it is true that

$$h(\mathbf{X}) \leq f(\mathbf{X}) \leq g(\mathbf{X}) \tag{19}$$

with the *concave* quadratic function

$$h(\mathbf{X}) = a_l + 2\Re\{\langle \bar{X}\mathbf{X}^H \rangle\}/\sigma - \langle \mathcal{B}_l, (\mathbf{X})^2 \rangle/\sigma \tag{20}$$

and the *convex* quadratic function

$$g(\mathbf{X}) = a_u + \langle \mathcal{B}_u, (\mathbf{X})^2 \rangle/\sigma \tag{21}$$

where $a_l \triangleq f(\bar{X}) - \langle (\bar{X})^2 \rangle/\sigma$, $0 \preceq \mathcal{B}_l \triangleq \sigma^{-1} I_m - (\sigma I_m + (\bar{X})^2)^{-1}$, and $a_u \triangleq f(\bar{X}) + \langle (I_m + (\bar{X})^2/\sigma)^{-1} - I_m \rangle$, $0 \prec \mathcal{B}_u \triangleq (I_m + (\bar{X})^2/\sigma)^{-1}$. Both functions h and g agree with f at $\bar{X}$.

Proof. Due to space limitations, we provide only a sketch of the proof. Rewrite $f(\mathbf{X}) = -\ln |I_m - (\mathbf{X})^2/((\mathbf{X})^2 + \sigma I_m)^{-1}|$, which is convex as a function in $((\mathbf{X})^2, (\mathbf{X})^2 + \sigma I_m)$ [18]. Then $h(\mathbf{X})$ defined by (20) actually is the first order approximation of this function at $((\bar{X})^2, (\bar{X})^2 + \sigma I_m)$, which is its minorant at $((\bar{X})^2, (\bar{X})^2 + \sigma I_m)$ [17], proving the first inequality in (19). On the other hand, considering f as a concave function in $(\mathbf{X})^2$, $g(\mathbf{X})$ defined by (21) is seen as its first order approximation at $(\bar{X})^2$ and thus is its majorant at $(\bar{X})^2$ [17], proving the second inequality in (19).

REFERENCES

[1] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory.*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.

[2] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Commun. Mag.*, vol. 19, no. 2, pp. 40–47, Feb. 2012.

[3] T. M. Hoang, T. Q. Duong, H. A. Suraweera, C. Tellambura, and H. V. Poor, "Cooperative beamforming and user selection for improving the security of relay-aided systems," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 5039–5050, Dec. 2015.

[4] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, "On the resilence of wireless multiuser networks to passive and active eavesdroppers," *IEEE J. Sel. Areas. Commun.*, vol. 31, no. 9, p. 1850, 2013.

[5] R. L. G. Cavalcante, S. Stanczak, M. Schubert, A. Eisenlatter, and U. Turke, "Toward energy-efficienct 5G wireless communications technologies," *IEEE Signal Process. Mag.*, vol. 13, no. 11, pp. 24–34, Nov. 2014.

[6] C. I, C. Rowell, S. Han, Z. Xu, G. Li, and Z. Pan, "Toward green and soft: A 5G perspective," *IEEE Commun. Mag.*, vol. 13, no. 2, pp. 66–73, Feb. 2014.

[7] O. Tervo, L.-N. Tran, and M. Juntti, "Optimal energy-efficient transmit beamforming for multi-user MISO downlink," *IEEE Trans. Signal Process.*, vol. 63, no. 20, pp. 5574–5588, Oct. 2015.

[8] Q.-D. Vu, L.-N. Tran, R. Farrell, and E.-K. Hong, "Energy-efficient zero-forcing precoding design for small-cell networks," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 790–804, Feb 2016.

[9] N. Zhao, F. R. Yu, and H. Sun, "Adaptive energy-efficient power allocation in green interference-alignment-based wireless networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 9, pp. 4268–4281, Sept. 2015.

[10] T. T. Vu, H. H. Kha, and H. D. Tuan, "Transceiver design for optimizing the energy efficiency in multiuser MIMO channels," *Commun. Lett.*, vol. 20, no. 8, pp. 1507–1510, Aug. 2016.

[11] W. Dinkelbach, "On nonlinear fractional programming," *Management Science*, vol. 13, no. 7, pp. 492–498, Mar. 1967.

[12] A. Kalantari, S. Maleki, S. Chatzinotas, and B. Ottersten, "Secrecy energy efficiency optimization for MISO and SISO communication networks," in *Proc. IEEE 16th Inter. Workshop on Signal Process. Advances in Wireless Commun.(SPAWC)*, 2015, pp. 21–25.

[13] A. Zappone, P.-H. Lin, and E. Jorswieck, "Energy efficiency of confidential multi-antenna systems with artificial noise and statistical CSI," *IEEE J. Selec. Topics Signal Process.*, vol. 10, no. 8, pp. 1462–1477, Aug. 2016.

[14] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Imporving wireless physial layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[15] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[16] C. Xiong, G. Y. Li, S. Zhang, Y. Chen, and S. Xu, "Energy-efficient resource allocation in OFDMA networks," *IEEE Trans. Commun.*, vol. 60, no. 12, pp. 3767–3778, Dec. 2012.

[17] H. Tuy, *Convex Analysis and Global Optimization (second edition)*. Springer, 2016.

[18] H. H. M. Tam, H. D. Tuan, and D. T. Ngo, "Successive convex quadratic programming for quality-of-service management in full-duplex MU-MIMO multicell networks," *IEEE Trans. Commun.*, vol. 64, pp. 2340–2353, Jun. 2016.